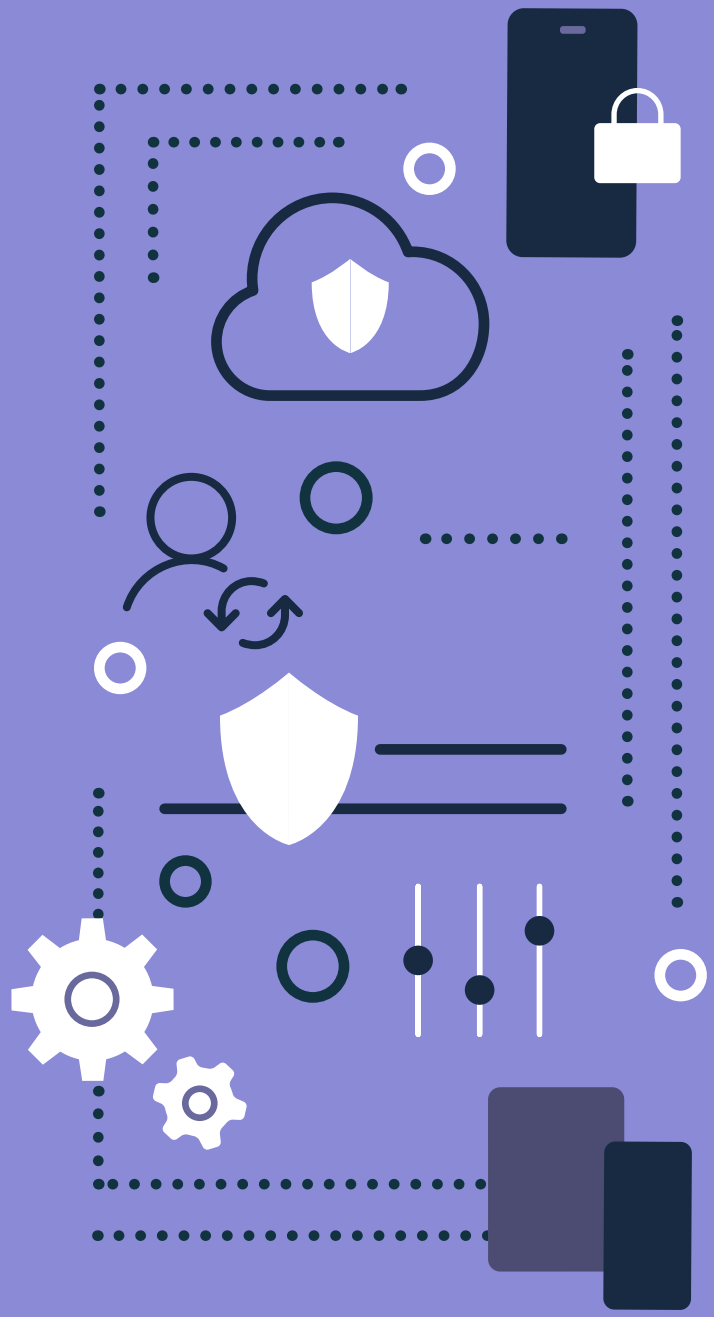


jamf

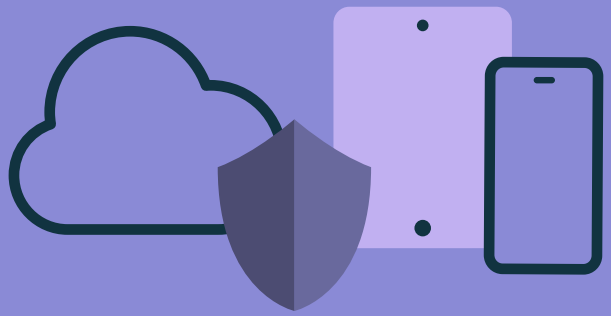
基礎ガイド

Mac向けウィルス対策

エンタープライズにおける Apple製品の利用が拡大し続けるなか、Macに特化したマルウェア対策の必要性が高まっています。

すべてのプラットフォームで脅威の検出が増加するなか、Appleは比較的よく健闘していると言えますが、マルウェアに限定した検出数は、標的がより絞られた他の脅威と比べると伸び悩んでいます。

組織がリモートワークやハイブリッドワークを採用するようになり、テクノロジーを取り巻く状況は劇的に変化しました。これに対し、マルウェアの作者や攻撃者たちは、マルウェアツールの適応範囲や規模を調整することで対応するようになりました。攻撃者が一度に複数の脅威を用いるため、攻撃は複雑さを増しています。また、自動化された攻撃も増加傾向にあり、生産性を高めるためにユーザが使用するコラボレーションツールにまで拡大しています。



このガイドでは以下の点について説明します。

- Macに特化したウィルス対策とは
- Macユーザを狙ったマルウェアの増加
- こうした傾向を理解することが個人データの保護にとって重要な理由
- Macを確実に保護するためにJamfが提供しているソリューション

Macに特化したウィルス対策

ほとんどの組織にとって、ウィルス対策はデバイスに最低ラインのセキュリティを確保する上で不可欠なものです。macOSには、XProtect、Gatekeeper、MRTといった基本的なウィルス対策機能が搭載されています。しかし、これらのツールはあまり定期的にアップデートされておらず、その働きについてもあまり可視化されていません。Macを狙ったマルウェアを阻止・検疫するために、組織はWindowsベースのソリューションがmacOSに提供できる範囲をはるかに超えた高度なウィルス対策機能を必要としています。
マルウェア、アドウェア、その他の迷惑なソフトウェアによって問題が発生してから対策を打つのでは遅すぎます。

Windowsを狙った脅威をMac上で探すのではなく、Macを狙った攻撃を効果的に検出し、修復してくれるウィルス対策を導入するのがベストです。デバイスのセキュリティやユーザエクスペリエンスの側面からも、効果的かつ効率的、そして包括的なMac向けの対策が必要になります。

Kaspersky Labの報告書によれば、プライバシーの侵害には、GPS座標の伝達や暗号化されたメッセージの解読・記録、通話の監視または録音など含む、数多くの行為が存在します。

変化する脅威

社会の危機的状況を利用したフィッシングキャンペーンが顕著に増加し、供給が減少したり世界的に不足している商品に関して個人が感じている不安や懸念を利用したものが特に増えています。これにはITサポートに関係した詐欺も含まれます。

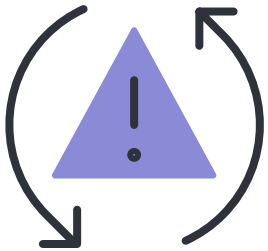
オンラインストーカー

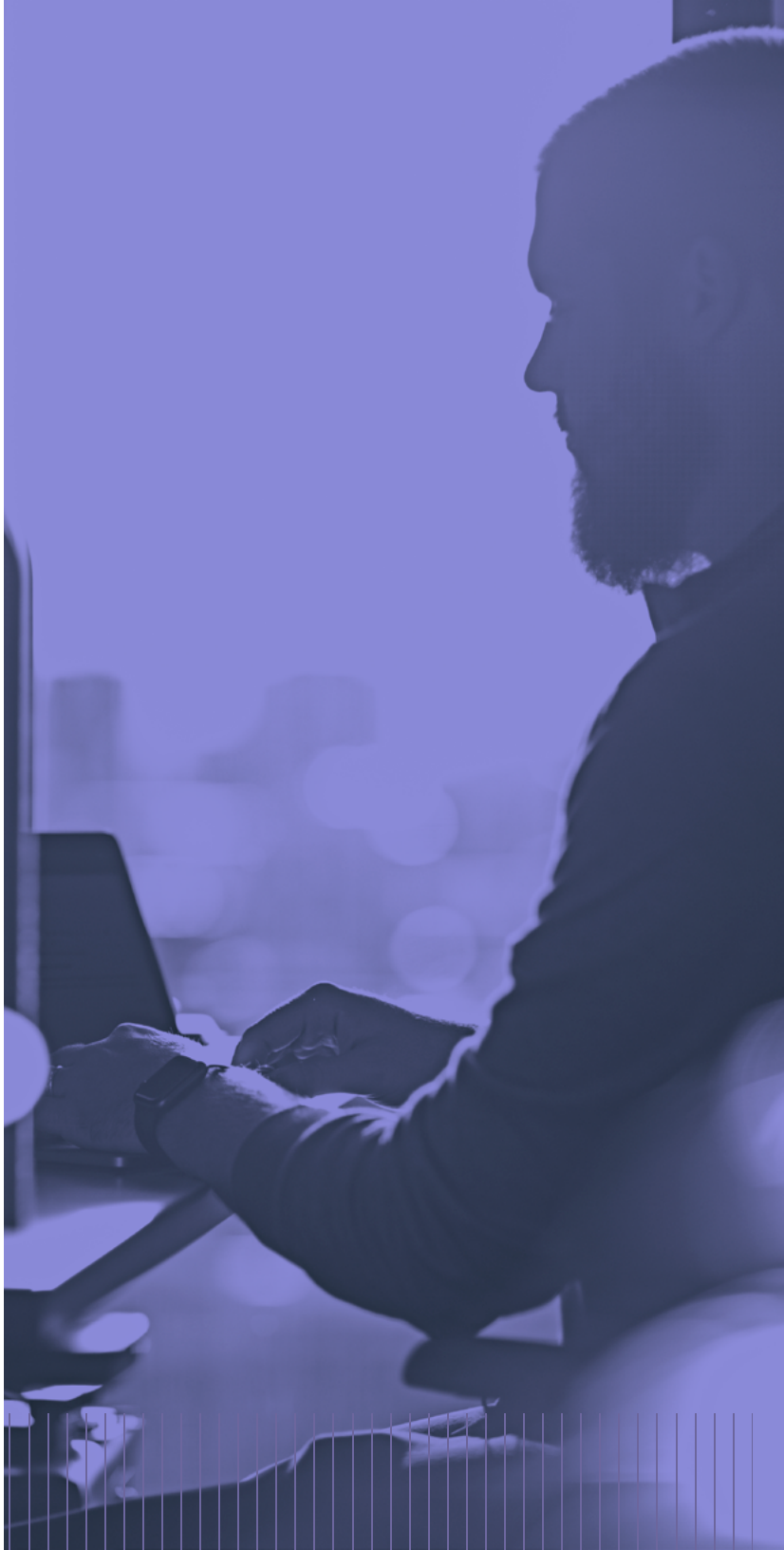
アドウェア、スパイウェア、ストーカーウェアは、いずれもユーザのデータを取得し、流出させるために使用されるマルウェアです。特にストーカーウェアは、個人を特定するあらゆるデータをリアルタイムで悪用するもので、「クリープウェア」としても知られています。

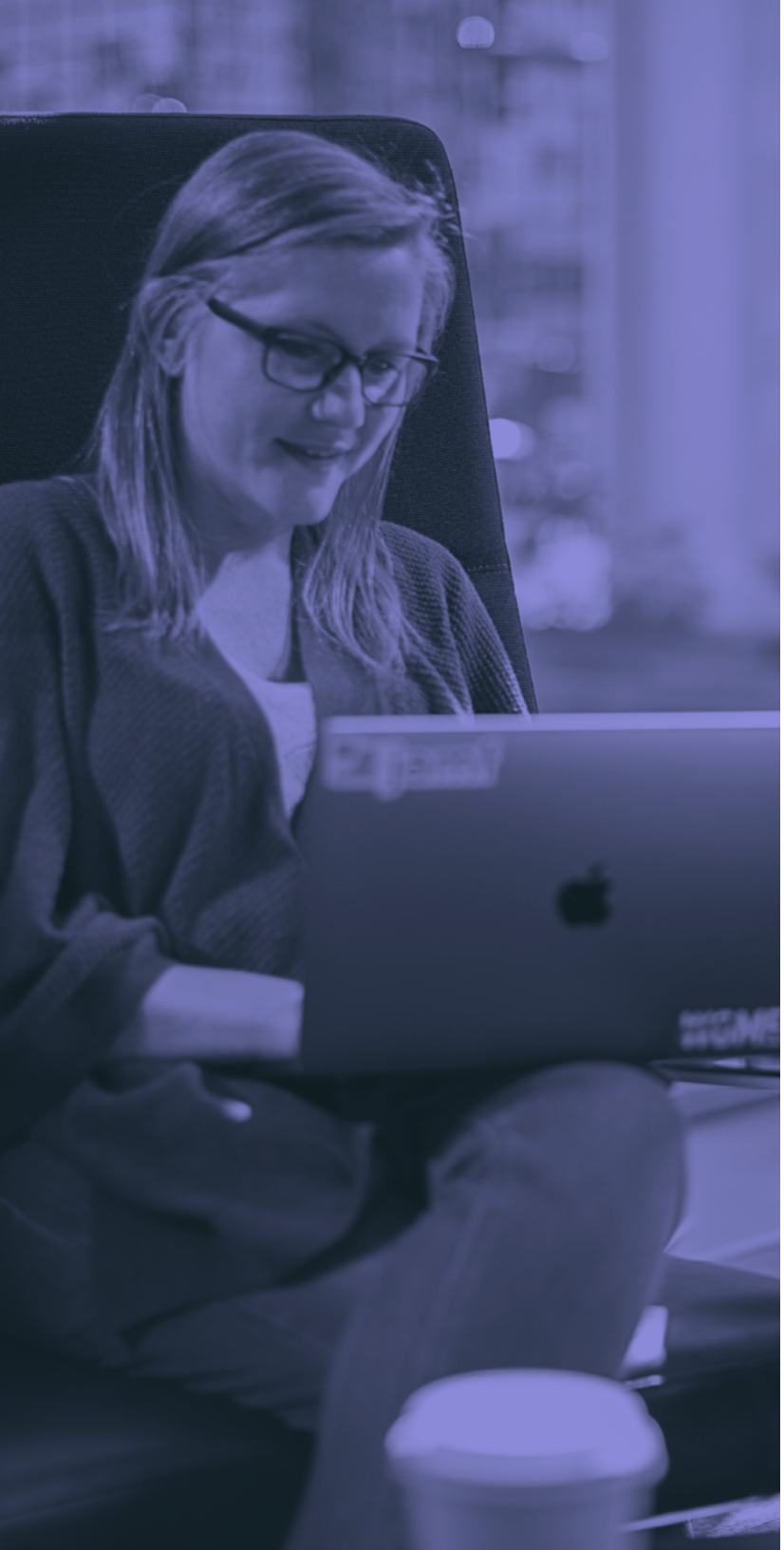
長期戦

このことを考える上で重要なのは、攻撃者が長期戦を仕掛けてくる場合が数多くあるという点です。つまり、彼らは攻撃を成功させるために必要なだけ時間をかける傾向にあります。また、1つのデバイスにマルウェアを1つだけ侵入させようとするのではなく、ありとあらゆる足がかりを利用して繰り返しアクセスを試み続けることもあります。このようにして時間を確保することで、戦略やツールを必要に応じて調整し、情報を十分に収集し、最終的にはマルウェアをシステムに深く潜り込ませることができるのです。

これは、ひとつの要素が次の要素に直接的に働きかけ攻撃を促進させる、循環的な手法といえます。







Macを狙うウィルスの現状

マルウェアは全般的に増加を続けており、AV-Test.orgによって2022年に特定されたマルウェアの総数は、PUA（望ましくない可能性のあるアプリケーション）を含め、12億2704万8144にものぼりました。ですが、Macユーザにとって良いニュースがあります。OSごとの分布を調べたところ、このうちmacOSを狙ったものは220個しか確認されなかったのです。

マルウェアの環境の変化には以下の要因が影響しています。

- 企業におけるAppleのマーケットシェアの継続的な拡大
- Apple製品の選択を可能にする従業員選択プログラムやBYODプログラムの存在
- リモートワークやハイブリッドワークへの世界的なシフトによって曖昧になった、かつてオフィスと自宅を分けていた境界線

喜ぶのは時期尚早です

このデータについて喜ぶべきことと考える人もいるかもしれません。しかし、さまざまなソースから収集されたテレメトリデータによると、プライベートで使用されるデバイスは、アドウェアを筆頭に、依然としてPUPにさらされていることがわかっています。

これは、職場における問題とはまったく異なるものですが、Macを使用する個人ユーザにとって、PUPやアドウェアはユーザの個人情報（PII）を狙う試みであり、下手をすれば、悪意のある広告によって個人データが追跡されたり、クリーニングソフトウェアを謳った怪しいアプリがダウンロードされたり、はるかに悪い事態につながる可能性もあります。

巧妙なマルウェア

Macを標的とした新型ランサムウェアが最後に検出されたのは数年前のことになりますが、2020年にはEvilQuest（別名ThiefQuest）というマルウェアの存在が明らかになりました。ランサムウェアのすべての要素を備えており、個人データや企業データを執拗に盗み出すという真の意図を隠すための単なる口実として、暗号化による「身代金」の要求を行います。

このようなマルウェアは、通常のソフトウェアと同様に時間とともに進化し、より大きな被害をもたらす機能が追加される一方で、検出を回避するために巧妙さを増していきます。デバイスを感染させた後、自らアップデートして進化することもあります。EvilQuestは現在進行形の脅威として、今後の変化に注意する必要があります。

進化し続ける脅威

「一時的に迷惑なだけ」と軽く考える人も多いアドウェア型マルウェアも、実は進化しています。Appleがリリースした最近のmacOSでは、アプリの起動を許可する前にアプリの署名を確認する仕組みになっています。これにより一部のマルウェア作者は、システム上の貴重なデータにアクセスするため、またインターネットの閲覧中に表示される広告を収益化するために、常識にとらわれない方法を必死で考えています。

これらの攻撃の例として、Safariアプリ自体を複製および改造し、不正な拡張機能をインストールしてユーザを追跡するものや、IT管理者がデバイス設定を管理するために使うものとよく似た構成プロファイルをユーザにインストールさせるもの、さらなる攻撃を行うために必要なアクセス許可を効果的に得るものなどが挙げられます。

また、アドウェアは危険性が低いと考えられていますが、macOSを狙ったもっとも一般的なマルウェアであると同時に、システムを感染させるためにもっとも革新的な手段を用いていること、さらに新しいマルウェアのペイロードをリモートで追加できる機能がますます一般化していることと相まって、その影響力を増しています。

スマートな戦略

残念ながら、私たちが直面している数々の脅威に対抗できる単一のソリューションは存在しません。ここで重要となるのが、脅威は毎回同じところからやってくるわけではない、ということです。攻撃者はその戦術を絶え間なく変化させ、彼らにとって最良の結果をもたらすデバイスやサービスを標的にします。彼らの勢いが止まるところを知らないのは、データによっても裏付けされている事実です。

このことは、仕事や普段の生活においてコンピュータに依存しているすべての人にとって、どのような意味を持つのでしょうか。一言で言えば、私たちに必要なのは襲ってくるあらゆる脅威をブロックし、未然に防ぎ、是正してくれるセキュリティ対策です。フィッシングのような一般的な脅威を見分ける方法を学んだり、知らないソフトウェアのインストールを避けるなど、警戒心を持ち続けることはセキュリティにおいて重要な意味を持ちます。

また、ITチームやセキュリティチームは、常に組織のセキュリティポスチャを強化し維持するために、油断を許さないワークフローを用意する必要があります。既知のシグネチャに基づいて脅威を検出するソフトウェアや、行動分析によって未知の脅威を事前に検出するヒューリスティック（発見的手法）を利用すると、組織を狙う脅威がどこからやってくるのかを理解できるだけでなく、その脅威から身を守る方法についても知識を得ることができます。

また、迅速かつ自動化されたインシデント対応を併用することで、検出された問題の修復を試みることも可能です。どちらも、攻撃の対象領域を最小化し、リスクを効率的に管理するのに役立つと同時に、深層防護の戦略に新たな側面を追加してくれます。

私たちは仕事を効率的にこなすためにMacを使っています。アプリを起動するたびに数千のコードをスキャンしてバグを探すことなど誰も望んでいません。だからこそ、Appleはユーザにとって極めてシンプルで使いやすい製品を提供することに全力を傾けているのです。私たちは、同じことがセキュリティソフトウェアにも当てはまると考えています。

Jamfの統合 & サポート

Jamf Protectは、シグネチャベースの検出と行動分析機能によりマルウェアや不審な行動を阻止・修復します。トップダウン型の詳細なインサイトにより、ITやセキュリティチームはデバイスのパフォーマンスに影響を与えている要因をセキュリティの観点から確認することができます。さらに、Jamf Proと組み合わせることで、パッチの一元管理や修復が可能になり、ありとあらゆる問題を解決することができます。これにJamf Connectを加えることで、トップクラスのセキュリティを実現させる3本柱が完成します。アイデンティティ&アクセス管理ソリューションを提供するJamf Connectは、クラウドベースのアイデンティティサービスを利用して、デバイスやリソースへのセキュアなアクセスを実現します。

Appleの内蔵ツールを含む深層防護戦略にJamfのパワーを集結させることで、素晴らしいユーザエクスペリエンスを提供しながら、デバイスに関する詳細なインサイトと分析を得ることができるため、Macのための効果的なセキュリティ体制を維持することができます。
このように階層化された戦略により、ITチームはデバイスやユーザデータを保護するために最適な判断を下すことができます。

エンタープライズにおけるApple製品の管理およびセキュリティのスタンダードであるJamfは、お客様の組織とユーザにとって最適なセキュリティ戦略を実現するための製品とソリューションを提供しています。

私たちはこれを「Trusted Access」と呼んでいます。**詳細はこちらから。**

私たちの言葉を鵜呑みにせず

実際にJamfのウィルス対策とエンドポイント保護を試してみてください。

急増する脅威や無数のマルウェアからMacフリートを保護し、不審な行動に対抗することに興味のある方は、ぜひ無料トライアルにお申し込みください。

無料トライアルに申し込む

もしくは、お近くの販売代理店までご連絡ください。

Jamf ProtectとMacのエンドポイント保護に関する詳細は、公式サイトをご覧ください。